

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

IN THE MATTER OF THE SEARCH OF

A DARK COLORED APPLE IPHONE AND
A LIGHT COLORED APPLE IPHONE,
CURRENTLY LOCATED AT THE
CHARLESTON COUNTY SHERIFF'S
OFFICE, 3691 LEEDS AVE, NORTH
CHARLESTON, SC 29405

Case No. 2:24-cr-692

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Robert Callahan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure, for a telephonic search warrant authorizing the examination of property – electronic devices – which are currently in law enforcement possession (the “Devices”), as described in Attachment A, and the extraction from that property of electronically stored information as described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and have been so employed since 2009. I have a Bachelor of Science degree in Criminal Justice received from the University of South Carolina. I am a graduate of the Federal Law Enforcement Training Center and the ATF National Academy. I am currently assigned to the ATF Charleston Field Office within the Charlotte Field Division. I have participated in numerous investigations involving state and federal firearm violations to include: the illegal possession of firearms, firearms trafficking, straw purchasing of firearms, dealing in firearms without a license, and firearms classified under the National Firearms Act (NFA), among others. I have also

participated in numerous investigations involving state and federal narcotics violations. Accordingly, I am thoroughly familiar with the investigative techniques used in these investigations, such as the use of undercover agents, the use of cooperating witnesses and confidential informants, surveillance, search and seizure warrants, and the extraction and analysis of data from digital devices. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that Christopher Lee HARRIS II and/or Emily Rose MORENO committed violations of Title 18 U.S.C. § 371 (conspiracy), Title 18 U.S.C. § 922(a)(6) (making of false statements in connection with the acquisition of a firearm), Title 18 U.S.C. § 922(g)(1) (felon in possession of a firearm), Title 18 U.S.C. § 922(g)(3) (unlawful user of a controlled substance in possession of a firearm) and Title 21 U.S.C. § 844(a) (unlawful possession of a controlled substance).

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is a dark colored Apple iPhone with a cracked back and front panel (may be a tempered glass screen protector) affixed with a case inscribed with, “Emily” (**Device 1**) and a light/pink colored Apple iPhone with a cracked back and front panel (may be a tempered glass screen protector) affixed with a clear case with black trim (**Device 2**),

collectively, the **Devices**. The **Devices** are currently located within the evidence department of the Charleston County Sheriff's Office, 3691 Leeds Ave, North Charleston, SC 29405.

6. The applied-for warrant would authorize the forensic examination of the **Devices** for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On July 16, 2024, at approximately 2:19 a.m. Deputy Stephen Gregg with the Charleston County Sheriff's Office was travelling north on Savannah Hwy near the 2700 block range when Deputy Gregg observed a dark colored sport utility vehicle travelling south on Savannah Hwy at a high rate of speed. Deputy Gregg activated his radar and confirmed the vehicle was driving one hundred and ten (110) miles per hour in a fifty-five (55) mile per hour zone. Deputy Gregg conducted a U-turn and attempted to catch up to the vehicle to conduct a traffic stop for the speeding violation. Deputy Gregg observed the vehicle turn onto Main Rd from Savannah Hwy and as the deputy approached the intersection, he activated the blue lights in his vehicle. After turning onto Main Rd, the deputy lost sight of the vehicle. Deputy Gregg pulled into the parking lot of a Waffle House where he observed a black Mercedes sport utility vehicle. Deputy Gregg observed the Mercedes accelerate through the parking lot where it turned back onto Savannah Hwy heading south. Deputy Gregg pursued the vehicle and observed the vehicle turn onto Bees Ferry Rd where it accelerated at speeds up to one hundred and thirty (130) miles per hour. The vehicle attempted to turn onto Ashley River Rd, however it failed to navigate the turn. The vehicle left the roadway and struck a tree where it came to rest adjacent to the roadway in a wooded area. Deputy Gregg indicated that the driver of the vehicle fled on foot.

8. As Deputy Gregg approached the vehicle, he observed a female in the front passenger seat, later identified as Emily Rose MORENO. Due to the collision and possible

injuries, MORENO was not removed from the vehicle until fire and emergency medical services (EMS) arrived on scene. While awaiting backup, Deputy Gregg asked MORENO if there were any firearms inside the vehicle and MORENO indicated that there was a firearm inside the vehicle. Once another law enforcement officer arrived on scene, Deputy Gregg retrieved a Romarm/Cugir Micro Draco, 7.62x39mm pistol with serial number 23PMD-50931 from the driver's side floorboard of the vehicle.

9. Upon the arrival of additional law enforcement personnel, they were able to approach the passenger side of the vehicle. Upon opening the front passenger side door, a deputy observed MORENO in the passenger seat and asked where the gun was and advised MORENO not to touch the gun. Another deputy indicated that one firearm had been removed from the vehicle but that they didn't know if there were more firearms inside the vehicle. The deputy then removed a black Inicat brand bag from around MORENO's neck and a black Coach brand bag from the passenger side floorboard at MORENO's feet due to the possibility that the bags could contain firearms. The two bags were placed on the ground outside the vehicle.

10. Upon fire and EMS arrival, MORENO was helped out of the vehicle. MORENO was in possession of a cell phone while being removed from the vehicle. Upon being placed on a stretcher for further evaluation, it appears at least one of the black bags was placed on the stretcher with MORENO. After being evaluated by EMS and refusing to be transported to the hospital, MORENO was observed wearing both black bags around her neck. MORENO was advised that she was being detained pending a search of the vehicle. The two black bags were eventually removed from MORENO by law enforcement, as well as **Device 1**. MORENO was observed utilizing **Device 1** during the incident prior to it being taken by law enforcement.

11. When asked who the driver of the vehicle was, MORENO stated she did not know the driver, did not know their name, and would not provide a description of the driver. MORENO stated they had just met at the bar that night and the unknown driver was operating her vehicle because she was intoxicated. MORENO indicated that it was just the driver and herself in the vehicle. When asked about firearms, MORENO stated she owns a “Glock” and a “Draco.” MORENO would later state that she would not answer any further questions without consulting with an attorney.

12. While MORENO was being attended to by EMS, a male and a female, believed to be the parents of Christopher Lee HARRIS, II, arrived on scene and inquired if their son was in the vehicle that had crashed and if he was ok. They indicated their son’s name is “Christopher Harris” and provided a physical description. Deputy Gregg asked them why they believed their son may have been in the vehicle and HARRIS’ mother indicated she had received a phone call and her son’s location observed on her cell phone indicated he was at the accident location. She told the deputy she had been attempting to call her son, but he was not answering his phone – which is why they arrived on scene. Deputy Gregg informed HARRIS’ parents there was only a female located in the vehicle. HARRIS’ mother asked if the female in the vehicle was “Emily” and stated that “Emily” is her son’s girlfriend and the two of them are always together. After being informed MORENO was the only individual found in the vehicle and that she was the passenger, HARRIS’ parents provided limited information and would not provide their son’s date of birth to law enforcement. HARRIS’ father stated, “I’m not sure my son was the driver, so I’m not trying to put my son in something that he’s not supposed to be in.” Deputy Gregg later asked HARRIS’

mother if HARRIS' location had moved at all, and she indicated that it had not. HARRIS' mother indicated that HARRIS may have multiple phones and "that's the only one he allows me to track".¹

13. A Charleston Police Department K-9 officer arrived on scene and conducted a track for the driver who fled from the vehicle, however no one was located.

14. Deputy Gregg conducted a search of the two black bags that were originally removed from the vehicle and then removed from MORENO's person. In the Coach brand bag, the deputy located a digital scale containing a white powder residue; a plastic bag containing approximately 1.6 grams of a white powder substance that field tested positive for cocaine; a loaded Glock, model 22, .40 caliber pistol with serial number EWG173US; a loaded Glock, model 19, 9mm pistol with serial number BSWY995, two additional firearm magazines; and mail bearing the name Christopher Lee Harris II. In the Inicat brand bag, the deputy located approximately \$837.00 in U.S. currency; a loaded Glock, model 43X, 9mm pistol with serial number AHUX834; an additional firearm magazine; **Device 2**, documents bearing MORENO's name and a Chevrolet car key.

15. The Mercedes was pulled out of the tree line and loaded onto a tow truck. Deputy Gregg searched the vehicle and did not seize any additional items from the vehicle prior to it being towed. MORENO was arrested and charged with possession of cocaine. MORENO was read her Miranda rights and indicated she did not wish to speak to law enforcement. MORENO was

¹ "Find My" is an application utilized on Apple iPhones and when "Share My Location" is turned on, you can share your location with friends, family, and contacts from your iPhone or iPad with "Find My." If you and the person you share your location with both have an iPhone with iOS 15 or later, you share your "Live Location" – so that your friends or family members can see your location in real time.

ultimately booked into the Charleston County Detention Center after being cleared from the hospital.

16. I queried HARRIS in the South Carolina Department of Motor Vehicles website and discovered HARRIS' listed address to be 615 Tribeca Ct, Charleston, SC 29414. I viewed a map of the collision location in comparison with HARRIS' address and discovered them to be approximately 2.8 miles apart as a vehicle would travel and approximately 1.61 miles apart in a straight line according to Google Earth metrics.

17. I queried the license plate of the aforementioned Mercedes (SC YBF865) that fled from deputies and discovered the lessee of the vehicle to be MORENO. Additionally, I queried HARRIS in the South Carolina Department of Motor Vehicles website for traffic tickets and discovered that on May 31, 2024 HARRIS received a traffic ticket for driving under suspension while operating the aforementioned Mercedes leased by MORENO. I also queried HARRIS in the South Carolina Department of Motor Vehicles website for vehicles and discovered that HARRIS is the listed owner of a 2022 Chevrolet Malibu, bearing SC license plate WYC452. Of note, a Chevrolet car key was located in the Inicat brand bag recovered in this incident.

18. The Charleston County Sheriff's Office entered the four (4) recovered firearms into e-Trace.² I reviewed the e-Trace summaries and discovered that the Romarm/Cugir pistol recovered from the driver's side floorboard was purchased by MORENO on May 6, 2024 (71 days

² The e-Trace application is a browser-based web application that allows participating law enforcement agencies to submit firearm traces to the ATF National Tracing Center via the internet. The application is used to trace the purchase and/or history of weapons from their original manufacturer or importer, through the wholesale/retail distribution chain, to the first person who bought them.

time-to-crime) from Palmetto State Armory. The Glock 43X pistol recovered from the Inicat brand bag was also purchased by MORENO on March 29, 2024 (109 days time-to-crime) from Palmetto State Armory. I also discovered the Glock 19 pistol recovered from the Coach brand bag was purchased by Tristan Maxwell Reed on July 7, 2021 (1,105 days time-to-crime) from Allied Arms. Of note, Reed's listed address of 615 Tribeca Ct, Charleston, SC 29414, is the same listed address for HARRIS.

19. The firearms were test-fired by the Charleston County Sheriff's Office and the casings were entered into the National Integrated Ballistic Information Network (NIBIN).³ In reviewing the entries, the test-fired casing from the Romarm/Cugir pistol generated a preliminary investigative lead indicating the firearm may be linked to a shooting that occurred on June 5, 2024, approximately thirty days after the firearm was purchased by MORENO. During the June 5, 2024 incident, deputies with the Charleston County Sheriff's Office responded to the area of County Line Rd and Hwy 165 in Ravenel, SC for a shots fired call at approximately 5:00 a.m. Upon arrival, the deputy met with the complainants who indicated they heard gunshots nearby and when they went outside to investigate, they observed an individual in a vehicle shooting at a stop sign across the street. Deputies then observed a stop sign that appeared to have bullet holes and a short distance away they recovered four spent 7.62x39mm shell casings in the area where the complainant indicated they observed the individual shooting.

³ The National Integrated Ballistic Information Network (NIBIN) is a national network that allows for the capture and comparison of ballistic evidence. Preliminary NIBIN leads are for investigative purposes only and is not a confirmed identification. For confirmation, a direct comparative microscopic examination of the evidence by a forensic services laboratory is required.

20. I spoke with Sgt. Gilbert Baldwin of the Charleston County Sheriff's Office, and he indicated on July 19, 2024, MORENO came to the front desk of the Sheriff's Office and attempted to retrieve keys, a cell phone, and a purse that were taken into custody by the Sheriff's Office associated with this case. Sgt. Baldwin stated no items were released and upon MORENO exiting the office, a light skinned black male, who the deputy believed to be HARRIS, requested the same items.

21. I also spoke with Master Deputy Derek Lee of the Charleston County Sheriff's Office, and he recalled that a day or two after the incident, MORENO came to the front desk of the Sheriff's Office and attempted to retrieve a bag and a cell phone. Master Deputy Lee stated no items were returned and shortly after MORENO left, HARRIS came to the front desk and attempted to retrieve keys and a cell phone. Master Deputy Lee stated HARRIS indicated he needed his keys to get to and from work.

22. I reviewed HARRIS' criminal history and obtained court records that indicate HARRIS was convicted of assault and battery 1st degree and discharging firearms into a dwelling with a sentence date of April 27, 2022. These crimes, committed in the state of South Carolina, are punishable by a term of imprisonment of over one year. Thus, HARRIS is prohibited from possessing firearms and ammunition for purposes of Title 18 U.S.C. § 922(g)(1). Per my knowledge, HARRIS has not received a pardon for his South Carolina convictions.

23. I obtained a South Carolina Department of Corrections Gun Control Act Form signed by HARRIS on August 22, 2022 in which HARRIS acknowledged that he is aware and understands how the Gun Control Act applies to him.

24. I am aware through training and experience and conferring with other Special Agents, to include ATF Interstate Nexus Experts that the firearms and a representative sample of the ammunition seized by the Charleston County Sheriff's Office did affect interstate commerce.

25. I know that cell phones, computers and other digital devices are often used by certain individuals to facilitate the commission of criminal acts. Specifically, I know that firearms and cell phones are tools of the drug trade. I know that certain individuals will often utilize multiple digital devices, acquire new devices, or discard devices to avoid detection. Further, I am aware that incriminating evidence is often located within text messages, as well as photos and videos contained on cell phones and within web activity and saved documents on computers, hard drives, and other internal and external storage devices. Additionally, call logs (for incoming, outgoing, and missed calls), stored contact lists, and location information have proven to be valuable evidence in criminal cases. I know that individuals involved in the drug trade utilize stash houses and other locations to hide evidence, and to meet suppliers, dealers, and customers. I know that individuals prohibited from possessing firearms or those individuals that want to conceal ownership of firearms, often utilize a straw purchaser to purchase firearms on their behalf from an FFL and that on occasion, the prohibited person will accompany the straw purchaser to the FFL. The revelation of these locations is valuable to an investigation and can aid in identifying possible co-conspirators. Moreover, I am familiar with technology, such as Cellebrite mobile data transfer equipment, that allows law enforcement investigators to harvest data (such as incoming and outgoing text messages, photos, videos, call logs, and contacts) from cellular telephones. I also know that cellular telephones are often used by individuals to conduct financial transactions during the unlawful procurement of firearms and controlled substances. I know that application such as banking institutions and third-party applications, such as "Cash App", can be installed on cellular

telephones which allow individuals to electronically transfer financial funds to other parties during the unlawful acquisition or straw purchasing of firearms as well as controlled substances. I know that individuals often have social media applications, such as Facebook, on their cellular telephones and oftentimes social media platforms are used as a method and means of communication during the unlawful procurement and dissemination of firearms and controlled substances. In addition, based on my experience, I know that individuals engaged in the illegal acquisition, possession, and dissemination of firearms and controlled substances often utilize mobile telephones and other digital devices to communicate with customers, receive orders, make purchases, create ledgers and bill of sale forms, and to arrange for dissemination of the firearms or controlled substances. Often times, photographs or videos are taken of the firearms and controlled substances to facilitate the transaction or to post the photographs and/or videos within social media applications or in online firearm classified advertisements. These photographs and videos can be maintained on cellular telephones, computers, and other digital devices. I also know that digital devices reveal evidence of user attribution, showing who used or owned the device at the time it was seized by law enforcement.

26. Based on my training and experience, as applied to the circumstances in this case, I know that evidence of user attribution, showing who used or owned the device, can help aid in identifying the identity of the driver of the vehicle that fled from law enforcement. I know that information contained in digital devices such as messages, documents, photos, videos, and financial transactions, can aid in determining firearm possession and if firearms were straw purchased. I also know that the aforementioned information contained in digital devices can indicate if controlled substances are being distributed, and if so, who is distributing them and from whom they are acquiring and to whom they are distributing the controlled substances.

27. The **Devices** are currently in storage at the Charleston County Sheriff's Office evidence department, 3691 Leeds Ave, North Charleston, SC 29405. In my training and experience, I know that the **Devices** have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the Charleston County Sheriff's Office.

TECHNICAL TERMS

28. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1) A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

c. A “tablet” is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. Internet Protocol (“IP”) Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service

providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. The “Internet” is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

g. “Internet Service Providers,” or “ISPs,” are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line (“DSL”), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

h. “Domain Name” means the common, easy-to-remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for

educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

i. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

29. Based on my training, experience, and research, I know that certain cell phones and tablets have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and sometimes by implication who did not, as well as evidence relating to the commission of the offenses under investigation.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the Devices, in whatever form they are found. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the Devices for at least the following reasons:

a. Individuals who engage in criminal activity, including the illegal purchase and

possession of firearms as well as the illegal purchase and possession of controlled substances use digital devices, like the Devices, to access websites to facilitate illegal activity and to communicate with co-conspirators; to store on digital devices, like the Devices, documents and records relating to their illegal activity, which can include order history, online communication, email, text or other “Short Message Service (“SMS”) messages, and photos; contact information of co-conspirators, including telephone numbers, email addresses and identifiers for social media accounts.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often “back up” or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The

browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

31. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion

of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other

forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

f. I know that when an individual uses a digital device to unlawfully acquire, posses, or sell firearms and controlled substances, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of the crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

32. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the

purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by

the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, “Hide It Pro,” disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

33. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

a. The digital devices, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

b. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic

storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

c. In searching the **Devices**, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the **Devices** will be specifically chosen to identify the specific items to be seized under this warrant.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

34. Because forensic examiners will be conducting their search of the **Devices** in a law enforcement setting over a potentially prolonged period of time, I respectfully submit that good cause has been shown, and therefore request authority, to conduct the search at any time of the day or night.

CONCLUSION

35. I submit that this affidavit supports probable cause for a warrant to search the **Devices** described in Attachment A and to seize the items described in Attachment B.

This affidavit has been reviewed by AUSA Carra Henderson.

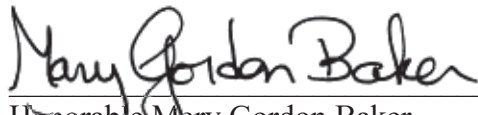
Respectfully submitted,

ROBERT CALLAHAN
Digitally signed by ROBERT
CALLAHAN
Date: 2024.08.16 11:03:54 -04'00'

Robert Callahan
Special Agent
Bureau of Alcohol, Tobacco, Firearms &
Explosives

SUBSCRIBED AND SWORN TO ME VIA
TELEPHONE OR OTHER RELIABLE
ELECTRONIC MEANS AND SIGNED
BY ME PURSUANT TO
FED. R. CRIM. P. 4.1 AND 4(D) OR 41(D)(3),
AS APPLICABLE.

This 16 day of August 2024



Honorable Mary Gordon Baker
United States Magistrate Judge